Habiendo tomado conocimiento de lo requerido por la Sección INFORMES mediante NO-2019-73436868-APN-SINFO#PFA, el cual guarda relación con lo requerido bajo NO-72377286-APN-DNPDP#AAIP por el Sr. Director Nacional de Protección de Datos Personales de la Agencia de Acceso a la Información Pública, mediante la cual hace referencia al incidente sucedido en la Fuerza consistente en la filtración de información de las Bases de Datos, y conforme las facultades conferidas por la Ley 25.326 y la Decisión Administrativa N° 1002/17, se deberá expedir sobre los siguientes puntos:

1-Indicar desde cuando se tiene conocimiento de la filtración de los datos y que medidas fueron adoptadas en consecuencia.

Respuesta:

Con fecha 12 de agosto del corriente, siendo las 10:40 hs. se toma conocimiento por intermedio de Sr. Director de CIBERCRIMEN del Ministerio de SEGURIDAD DE LA NACION, Lic. Pablo LASARO, que en la plataforma de la red social Twitter y posteriormente Telegram, mediante la cuenta @lagorraleaks, se habían efectuado diversas publicaciones donde los ciberdelincuentes habrían publicado en la red TOR (Deep-Web) 700 Gb de información de esta Policía Federal Argentina.

Ante tal magnitud, se conformó en el ámbito de la Sección CIBERSEGURIDAD un Comité de Crisis, conformado por el Sr. Superintendente FEDERAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES, Director General de INTELIGENCIA CRIMINAL, Director General de OPERACIONES TECNICAS, Jefe del Departamento TECNICO CONTRA EL NARCOTRAFICO, Jefe del Departamento TECNICO OPERATIVO, Jefe A/C del Departamento MOVIMIENTO DE PERSONAL, Director de INVESTIGACIONES CIBERCRIMEN de la Policía de la Provincia de Buenos Aires, Oficiales Jefes de las Distintas Áreas supuestamente alcanzadas.

Posteriormente, y ya teniendo identificado el tipo de información filtrada, la Sección CIBERSEGURIDAD estableció en principio, que unos de los vectores de ataque correspondieron a la intrusión de los ciberdelincuentes a diversas casillas de correos comerciales (Hotmail, Gmail) utilizadas por las dependencias policiales, mediante una técnica de Phishing que fuera detectada, reportada por esta Sección y mitigada con fecha 30/07/2019, por la Sección INFORMATICA de la Superintendencia de BIENESTAR, en razón de que en el sitio de la Página Oficial https://supbienestar.gob.ar se encontraba alojado un formulario malicioso que simulaba ser de un acceso al servicio de Onedrive para la descarga de un archivo, técnica utilizada por el ciberdelincuente para apoderarse de los nombres de usuarios y contraseñas de acceso, según se desprende de las comunicaciones efectuadas por dicha Sección mediante NO-2019-72311832-APN-SINF#PFA y NO-2019-73090818-APN-SINF#PFA.

El Departamento CIBERDELITO, al tomar conocimiento de este tipo de técnica de phishing judicializó la causa en la que interviniera el Juzgado Nacional en lo Criminal de Instrucción N° 6 a cargo de la Dra. María Alejandra PRIVITOLA, Secretaría N° 118 del Dr. Mariano FREIJO.

Asimismo, con fecha 30 de julio del corriente, esta Sección efectuó las comunicaciones de estilo a la Superioridad y se elaboró un Boletín Informativo N° 10, mediante el cual se explicó la maniobra del engaño, se efectuaron las recomendaciones del caso, como ser el cambio urgente de contraseñas para las dependencias que pudieran haber ingresado al sitio malicioso y la obligatoriedad del uso del correo electrónico Institucional para garantizar la veracidad y confidencialidad de la información, entre otras, para conocimiento de la totalidad de las dependencias de esta Institución.

Una vez determinada en forma parcial la metodología de ataque empleada que ocasionara la fuga de información Institucional, se advirtió a la totalidad de las áreas de la POLICIA FEDERAL ARGENTINA, a través de las Divisiones GESTION ADMINISTRATIVA de la amenaza en cuestión, con la finalidad de que la totalidad de las dependencias de cada área proceda en forma urgente al cambio de contraseña de las cuentas de correo electrónico, servicios de almacenamiento en la nube, conexiones WI-FI, y cualquier otro dispositivo que precise credenciales para su acceso. En el mismo sentido, se retransmitió mediante la plataforma del Sistema de Mensajería Electrónica SAFWIN y correo electrónico Institucional, directivas con respecto a cambio de contraseñas de los servicios enunciados anteriormente, como así también en forma indefectible se proceda a la habilitación de un doble factor de autenticación para garantizar un acceso seguro.

En este contexto, el día martes 13 de agosto, se conformaron equipos de trabajo permanentes integrados por profesionales en la materia de ciberseguridad, peritos informáticos, analistas de sistemas y técnicos, entre otros. Dentro de las divisiones de tarea, se crearon grupos de análisis de la información, sanitización de equipos y redes informáticas, detección y alerta temprana de incidentes, y de contacto para evacuar cualquier tipo de consultas relacionadas con seguridad de la información para todas las dependencias policiales, que así l requerían.

Ese mismo día, a partir del análisis de la información obtenida hasta ese momento, y habiendo identificado algunas de las áreas afectadas por la fuga de datos, por disposición de la superioridad, se brindó una charla informativa y de concientización a la Plana Mayor de la institución en el auditorio de la Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, donde se expusieron las técnicas de ataque, las áreas comprometidas, el tipo de información comprometida y el avance de las tareas de análisis que venía desarrollando la Sección CIBERSEGURIDAD.

El día miércoles 14 de agosto, se conformó una reunión del COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, integrada por Oficiales Superiores y Jefes de las principales áreas específicas, donde se expuso entre los presentes los hechos de conocimiento público, a los fines de analizar la cuestión y realizar recomendaciones para mitigar estos sucesos. En esa inteligencia, el Comité elaboro un documento "Normas de Seguridad Informática" con reitero de objetivos inmediatos y a futuro que eviten la fuga de información Institucional.

Con fecha 15 de agosto, el COMITÉ DE SEGURIDAD DE LA INFORMACIÓN convocó a los representantes de todas las áreas de la Policía Federal Argentina, en la que se puso en conocimiento de los de los avances y pormenores del ciberataque, se instrumentó la designación de un oficial de enlace permanente para transmitir o recibir comunicaciones vinculadas a la problemática en cuestión. También se consolidaron los lineamientos de seguridad oportunamente

comunicados, en especial el reitero de la prohibición del uso de cuentas de correo comerciales para el manejo de información institucional.

Ese misma fecha, se enviaron comunicaciones oficiales por el sistema de gestión documental electrónica (GDE), informando a las Divisiones GESTIÓN ADMINISTRATIVA de todas las Superintendencias, a los efectos de advertir mediante listados de Excel embebidos, cuáles eran las dependencias que fueron comprometidas, al mismo tiempo que se reiteraron las medidas de seguridad que deben implementar (backup, escaneos de malware, entre otras) con la finalidad de resguardar toda la información de la dependencia, y, en caso de ser necesario, se proceda a la contención del equipo informático aislándolo de la red e internet.

Posteriormente, con fecha viernes 16 de agosto se convocó a los representantes de cada superintendencia y se los puso en conocimiento de las directivas de buenas prácticas dispuestas por el Comité de SEGURIDAD DE LA INFORMACION en lo relativo a las medidas a implementar en las distintas dependencias de esta Institución.

Con fecha 20 de agosto del corriente año, por disposición del Sr. Superintendente FEDERAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES, mediante comunicación a través del sistema de gestión documental electrónica (DGE), NO-2019-74615248-APN-SFTIYCDGA#PFA, comunica las "Normas de Seguridad Informática para su más estricto cumplimiento", entre las que se reitera el solo uso del correo electrónico Institucional bajo el dominio @policiafederal.gov.ar; la prohibición del almacenamiento de datos en la nube (OneDrive/Google Drive), entre otros.

Con fecha 22 de agosto del corriente, la Sección CIBERSEGURIDAD, tomó conocimiento de un ataque de malware tipo ransomware que involucró equipos informáticos de la Fiscalía de Estado Bonaerense, por lo que se procedió a realizar e informar mediante Boletín Informativo N° 13 a la totalidad de las áreas de la Institución, mediante correo electrónico y a través del Sistema GDE.

El día 23 de agosto, la Dependencia antes mencionada, realiza un informe para concientizar al personal respecto a la amenaza de los ataques de ransomware y la forma de cómo prevenirnos, el cual se distribuye mediante el sistema GDE.

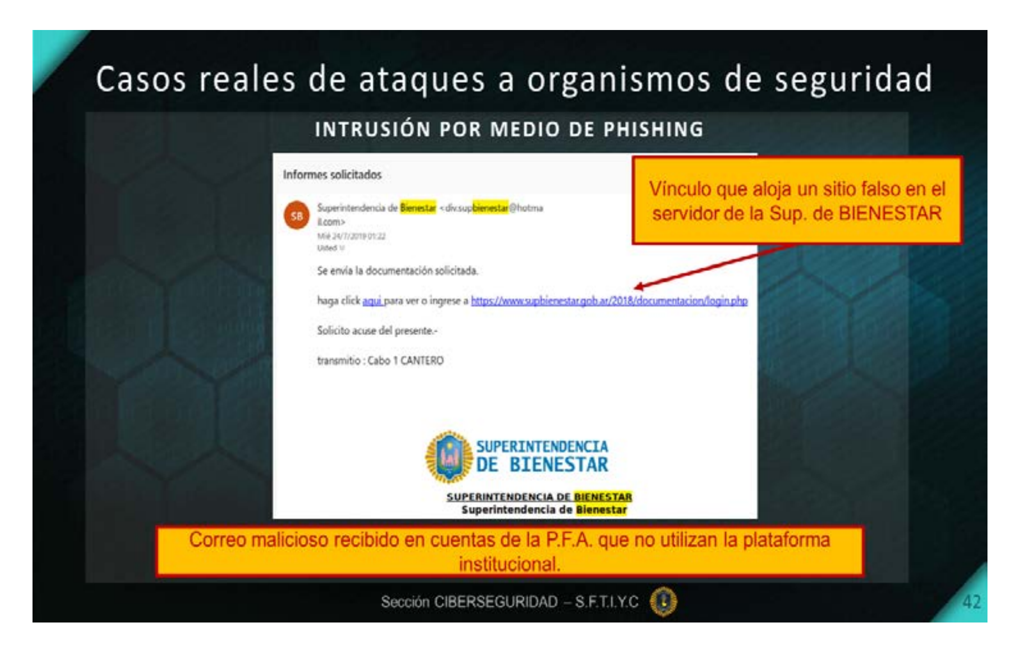
El lunes 26 de agosto del corriente, 18:15 hs. se realiza en el Auditorio de esta Superintendencia, una reunión con los referentes técnicos de las áreas de JEFATURA, SUBJEFATURA, Superintendencias de BIENESTAR, POLICIA CIENTIFICA, PERSONAL INSTRUCCIÓN Y DERECHOS HUMANOS, Direcciones Generales de INTELIGENCIA CRIMINAL, APLICACIONES TECNOLOGICAS, TECNOLOGIAS DE LA INFORMACIÓN, Departamento SISTEMAS CONTRA EL NARCOTRAFICO, Divisiones TECNOLOGIA APLICADA, ANALISIS Y PROSPECTIVA DEL NARCOTRAFICO, CENTRO DE ENTRENAMIENTO TECNOLOGICO, COMPUTACIÓN, TELEPROCESOS, Sección CIBERSEGURIDAD y Personal de la empresa de seguridad informática ESET. La misma se desarrolló en tres etapas:

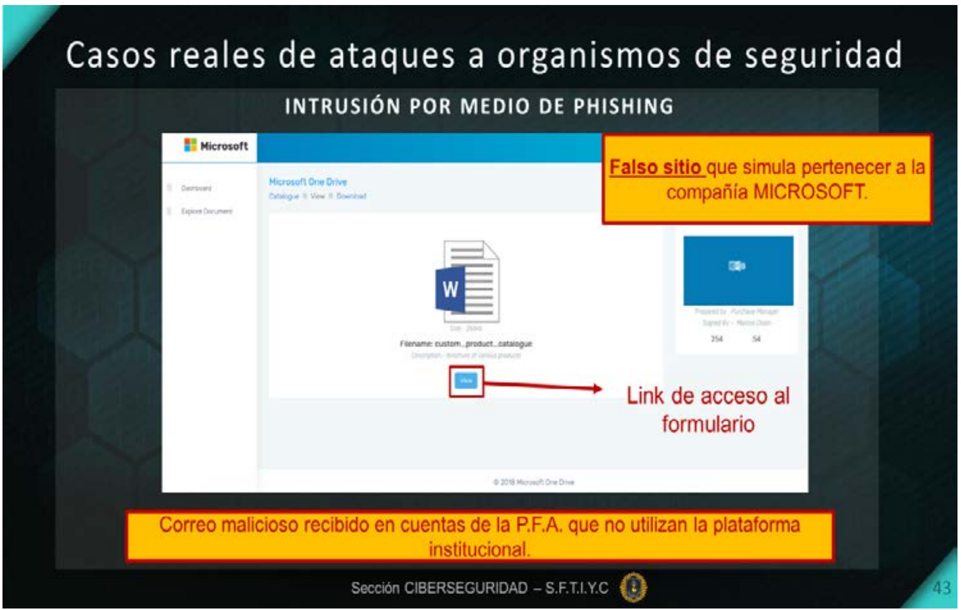
1era Etapa: La Sección CIBERSEGURIDAD interiorizó a los presentes, de la magnitud de los acontecimientos recientes que pusieron en manifiesto las falencias de seguridad informática que se presentaron en las distintas Áreas y Dependencias de esta Policía Federal Argentina, a través de una presentación PowerPoint.

2da Etapa: Personal de la empresa ESET, describió el funcionamiento de sus soluciones que puedan mitigar estos tipos de amenazas y los beneficios que podría traer su implementación en los distintos sectores de esta Institución.

3ra Etapa: Se hizo un cierre de la reunión y se establecieron pautas de trabajo con respecto al desarrollo e implementación de Software, como así también, recomendaciones sobre la estructura de red de las Distintas áreas.

Parte de la presentación disertada por la Sección CIBERSEGURIDAD, puntualizando la metodología de ataque utilizada por los ciberdelincuentes:





Casos reales de ataques a organismos de seguridad

INTRUSIÓN POR MEDIO DE PHISHING

Microsoft

Falso formulario que al completarlo le entrega el correo y su contraseña al delincuente

Correo malicioso recibido en cuentas de la P.F.A. que no utilizan la plataforma institucional.

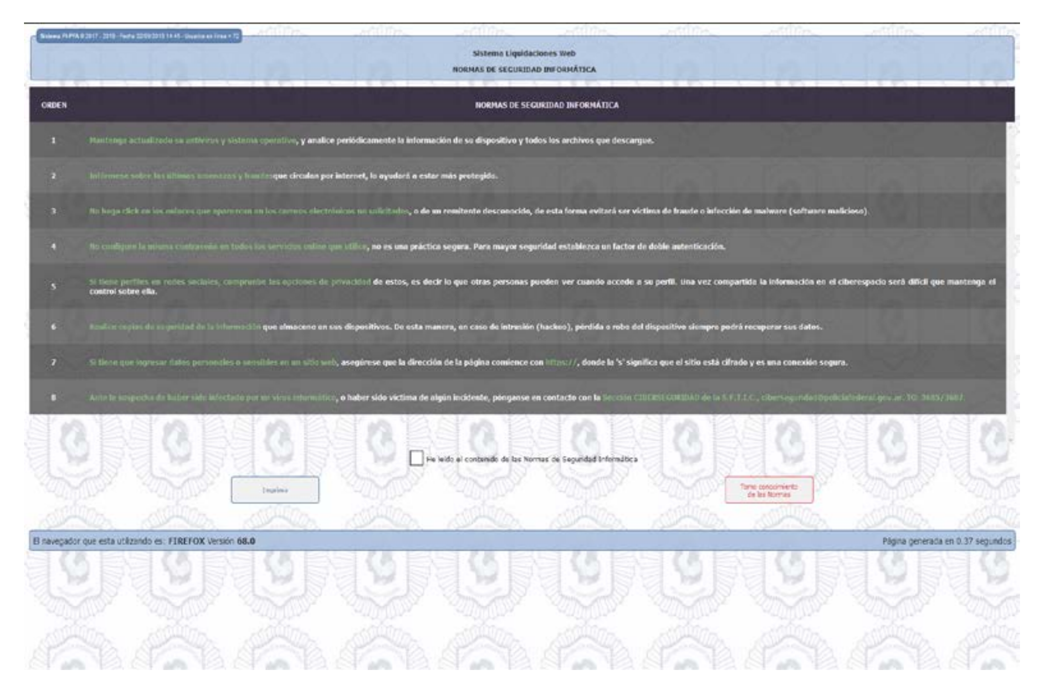
Sección CIBERSEGURIDAD – S.F.T.I.Y.C

44

El martes 27 de agosto, la Sección referida, procedió al dictado de una academia alineada con la campaña de concientización que ya se venía realizando durante el año 2018 y 2019 al personal de esta Institución en sus distintos cuadros, Jerarquías y escalafones. Los temas tratados, fueron incluidos como temario obligatorio para la próxima academia que a nivel Institucional se realizan en todas las Dependencias los últimos jueves de cada mes.

En horas de la tarde del mismo 27 de agosto, la División COMPUTACION desarrolló y habilitó a través del Portal PIPFA, una ventana emergente donde se dispone algunas de las Normas de Seguridad Informática, para que de forma obligatoria la totalidad del personal de esta Institución lea y comprenda las mismas. Estas se van a ir modificando en forma periódica y se publicarán con la misma metodología.

Captura de Pantallas Normas de Seguridad Informática



Sistema Liquidaciones Web

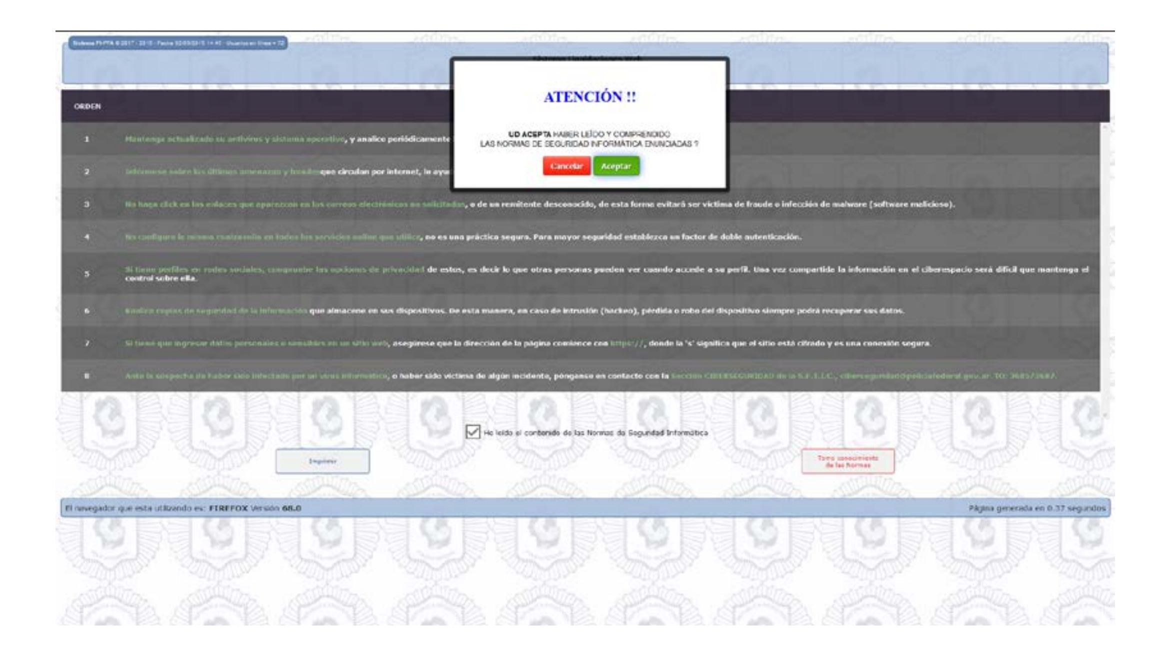
NORMAS DE SEGURIDAD INFORMÁTICA

ORDEN	NORMAS DE SEGURIDAD INFORMÁTICA
1	Mantenga actualizado su antivirus y sistema operativo, y analice periódicamente la información de su dispositivo y todos los archivos que descargue.
2	Infórmese sobre las últimas amenazas y fraudes que circulan por internet, lo ayudará a estar más protegido.
3	No haga click en los enlaces que aparezcan en los correos electrónicos no solicitados, o de un remitente desconocido, de esta forma evitará ser víctima de fraude o infección de malware (software malicioso).
4	No configure la misma contraseña en todos los servicios online que utilice, no es una práctica segura. Para mayor seguridad establezca un factor de doble autenticación.
5	Si tiene perfiles en redes sociales, compruebe las opciones de privacidad de estos, es decir lo que otras personas pueden ver cuando accede a su perfil. Una vez compartida la información en el ciberespacio será difícil que mantenga el control sobre ella.
6	Realice copias de seguridad de la información que almacena en sus dispositivos. De esta manera, en caso de intrusión (hackeo), pérdida o robo del dispositivo siempre podrá recuperar sus datos.
7	Si tiene que ingresar datos personales o sensibles en un sitio web, asegúrese que la dirección de la página comience con https://, donde la 's' significa que el sitio está cifrado y es una conexión segura.
8	[illegible], o haber sido víctima de algún incidente, póngase en contacto con la [illegible]

He leído el contenido de las Normas de Seguridad Informática

El navegador que esta utilizando es: FIREFOX Versión 68.0

Página generada en 0.37 segundos



Con respecto a la concientización en temas relacionados con la Seguridad de la Información, durante el año 2018 y 2019 se han dictado diferentes disertaciones, incluso se ha incorporado al Plan Anual de Capacitación DOS (02) Cursos "Introducción a la Seguridad de la Información", siendo realizado uno de ellos en el mes de marzo del corriente y otro en el mes de agosto, al cual han asistido representantes de las distintas fuerzas Federales.

A raíz de lo sucedido se intensificó la cantidad de disertaciones, con el fin de que el personal tome conciencia de los riesgos a lo que se está expuesto con el uso de las Tic´s y las distintas amenazas cibernéticas que cada día se vuelven más complejas con el avance de la tecnología.

Cabe aclarar que, de momento, las implementaciones llevadas a cabo para mitigar este tipo de amenazas fueron realizadas por dependencias técnicas específicas en la materia, no ocasionando erogación alguna para la Institución.

2) Informar cuales fueron las fallas de seguridad que posibilitaron dichas filtraciones

Respuesta:

Para determinar a ciencia cierta cuales fueron las fallas que posibilitaron la fuga de información, se solicitó mediante sistema Gestión Documental Electrónica a las áreas de PERSONAL, DROGAS PELIGROSAS y BIENESTAR a los efectos de que estas amplíen los motivos que dieran origen a la misma, por ser las dependencias propietarias de los datos personales filtrados, mediante NO-2019-75852101-APN-SCIB#PFA.

Cabe aclarar que la información que fuera afectada **NO** corresponde a datos de las bases que concentra los principales servicios informáticos que utiliza esta Policía Federal Argentina, las cuales se encuentran almacenadas en Servidores del Centro de Cómputos de la División

COMPUTACION, sino que pertenecen a datos descentralizados administrados localmente por las áreas anteriormente mencionadas.

Según se desprende de lo informado por la Superintendencia de Bienestar, a través de la Sección INFORMATICA mediante NO-2019-73090818-APN-SINF#PFA que textualmente refiere:

"El día 31 de Julio de corriente año se tomó conocimiento a través de un llamado telefónico del Subcrio VITTUZI, jefe de le Sección Ciberseguridad de la Superintendencia Federal de la Información y las Comunicaciones, de un e-mial enviado de la casilla div.supbienestar@hotmail.com (ajena a esta superintendencia) invitando a los usuarios a ingresar y completar un formulario alojado en nuestra web (www.supbienestar.gob.ar) con el fin de descargar un archivo. El mismo se trataba de un formulario fraudulento que simulaba ser el loguin de One Drive. Inmediatamente se procedió a eliminarlo de nuestra página ya que se comprobó que estaba recopilando correos y contraseñas en forma malintencionada.

El día 12/08 se nos alertó de un "Hacker" que había publicado información personal de los afiliados de esta Policía Federal en la Deep Web.

De inmediato se corroboró de dónde provenía dicha información. Se trata de datos del personal que se obtuvo en formato ".pdf" de los afiliados de la obra social fue realizada mediante un sistema de consulta que fue desarrollado por esta sección (Https://portal.supbienestar.gob.ar/gestion_angel). El mismo se encuentra publicado con el fin de que los anexos del interior puedan consultar el padrón y desempeñar sus funciones en base a esto, solo funciona a modo informativo, es decir, no posee permisos de escritura ni modificación sobre el padrón.

Notamos que la descarga del padrón no se realizó a la fuerza si no que, por el contrario, el ingreso se estableció con usuario y contraseña validos dentro del mismo, las descargas comenzaron el 12 de agosto de 2019 a las 01:15 am en adelante desde la ip de origen 93.188.163.28 que se encuentra asignada al proveedor Hostinger International y a su vez la ip se localizó en la cuidad de Greenville de carolina del sur (E.E.U.U.).

Por otra parte, se habían publicado contraseñas de muchos mails institucionales de esta superintendencia y pudimos concluir que esta información fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmamil. Se estableció que se aprovechó de la información obtenida para poder conseguir acceso a mencionado portal del cual se obtuvo la información publicada.

Según lo informado por la Superintendencia Federal de DROGAS PELIGROSAS, a través del Departamento SISTEMAS CONTRA EL NARCOTRAFICO, donde textualmente reza:

"Respecto a cuales fueron las fallas de seguridad que posibilitaron dichas filtraciones: a) No se cuenta con recursos técnicos y humanos con capacidad para determinar dicha solicitud. b) Se desconocen la totalidad de los datos filtrados, por ende no se puede determinar que se hayan obtenido de esta Superintendencia.

Referente al segundo punto "Detallar que tipo y cantidad de datos personales fueron comprometidos" del Departamento informa, que no se puede determinar tipo y cantidad de datos comprometidos, puesto que no se cuenta con la totalidad de la información compartida en Internet.

No obstante ello, esta Superintendencia viene aplicando políticas de seguridad a fin de evitar esta clase de filtraciones o al menos minimizar la posibilidad que suceda, como ser:

- Cambio de contraseñas cada determinado tiempo

- Cambio de clave de las redes Wifi

- Se promueven diferentes charlas con el personal a fin que tomen conocimiento sobre los peligros de abrir correos no deseados o links que deriven a páginas web desde mails ya sean conocidos o no.

- Se realizan backup periódicos de la información sensible.

Luego del incidente de público conocimiento, se extremaron las medidas de seguridad informáticas como ser:

- Para comunicaciones INSTITUCIONALES se utiliza únicamente el correo de POLICIA FEDERAL bajo el dominio (@policiafederal.gov.ar). Se prohíbe el uso de cualquier otro correo. El correo institucional se encuentra alojado en servidores de esta POLICIA FEDERAL ARGENTINA y se encuentra segurizado mediante una doble validación.

- La información sensible institucional, judicial y de los Recursos Humanos debe estar almacenada en forma SEGURA (encriptada y con contraseña) en las computadoras y/o servidores de las Áreas y Dependencias."

Respecto al área de la Superintendencia de PERSONAL, INSTRUCCIÓN Y DERECHOS HUMANOS, a través de su División PERSONAL SUPERIOR, al día de la fecha no se obtuvo respuesta alguna.

Reunida parte de la información y de acuerdo a las intervenciones del personal técnico de esta Sección, visualizando la información subida por los ciberdelincuentes a la Internet profunda (Deep Web) se puede concluir que las fallas que posibilitaron la filtración de los datos, son atribuidas en un principio al aprovechamiento y explotación de una vulnerabilidad del servidor web administrado por el área de Bienestar lo que ocasionara el alojamiento de un formulario malicioso para ser utilizado mediante la técnica de ingeniería social (Phishing) y obtener las credenciales de acceso a las cuentas de correo no institucionales utilizadas por las dependencias de la esta Policía Federal Argentina y el robo de las fichas en formato ".PDF" de los afiliados a la obra social.

Como segundo factor se debió a una falla humana por parte de los operadores de las cuentas no institucionales que fueran alcanzadas por el correo phishing y que permitió al ciberdelincuente obtener acceso total al servicio de correo tanto de Gmail y Hotmail y la descarga de la información que cada cuenta tenía almacenada en la nube, como ser servicio de OneDrive y Google Drive, que involucrara a Dependencias del área de SUBJEFATURA, Superintendencias Federal de DROGAS PELIGROSAS, PERSONAL, INSTRUCCIÓN Y DERECHOS HUMANOS y AGENCIAS Y DELEGACIONES FEDERALES.

Y como tercer factor de ataque, tras el análisis de esta Sección CIBERSEGURIDAD de los archivos de la Deep Web, se determinó que gran parte de los archivos que se filtraron corresponde a información almacenada en tres terminales informáticas utilizadas por la División PESONAL SUPERIOR, las cuales pudieron haber sido comprometidas por el Ciberdelincuente con una

infección de malware que permitiera el acceso total a los datos allí alojados en los discos rígidos, ya que se corroboró que esta Dependencia no utilizaba el almacenamiento de datos en la nube.

Cabe aclarar que la División OBTENCION DE EVIDENCIA DIGITAL del Departamento CIBERDELITO, realizó imagen forense de los discos afectados y se encuentra en etapa de análisis e investigativa, causa que pasara al fuero Federal e interviniera el Juzgado Nacional en lo Criminal y Correccional Federal N° 9 a cargo del Dr. Luis Osvaldo RODRIGUEZ, Secretaría N° 18 del Dr. Juan Manuel GRANGEAT. Causa N° C-55276/19 Caratulada "N.N S-VIOLACION DE CORRESPONDENCIA"

3) Detallar que tipo y cantidad de datos personales fueron comprometidos

Respuesta:

El área de Bienestar informó: Los datos comprometidos fueron: FICHAS PERSONALES DE LOS AFILIADOS, los cuales contienen los siguientes datos DNI, APELLIDO Y NOMBRE, N° AFILIADO, SEXO, ESTADO CIVIL, FECHA NACIMIENTO, EDAD, TELEFONO FIJO Y MOVIL, EMAIL, DIRECCIÓN, JERARQUIA, SITUACION REVISTA, LEGAJO PERSONAL, DEPENDENCIA, CBU, N° CAJA DE RETIRO, correspondiente a 220 Mil fichas. Asimismo, se divulgaron 1.083 cuentas de correo electrónico bajo el dominio @supbienestar.gob.ar con sus respectivas contraseñas. Los Directorios subidos en la Deep Web se identifican como "INFORMACION PERSONAL, OTRAS BASES DE DATOS".

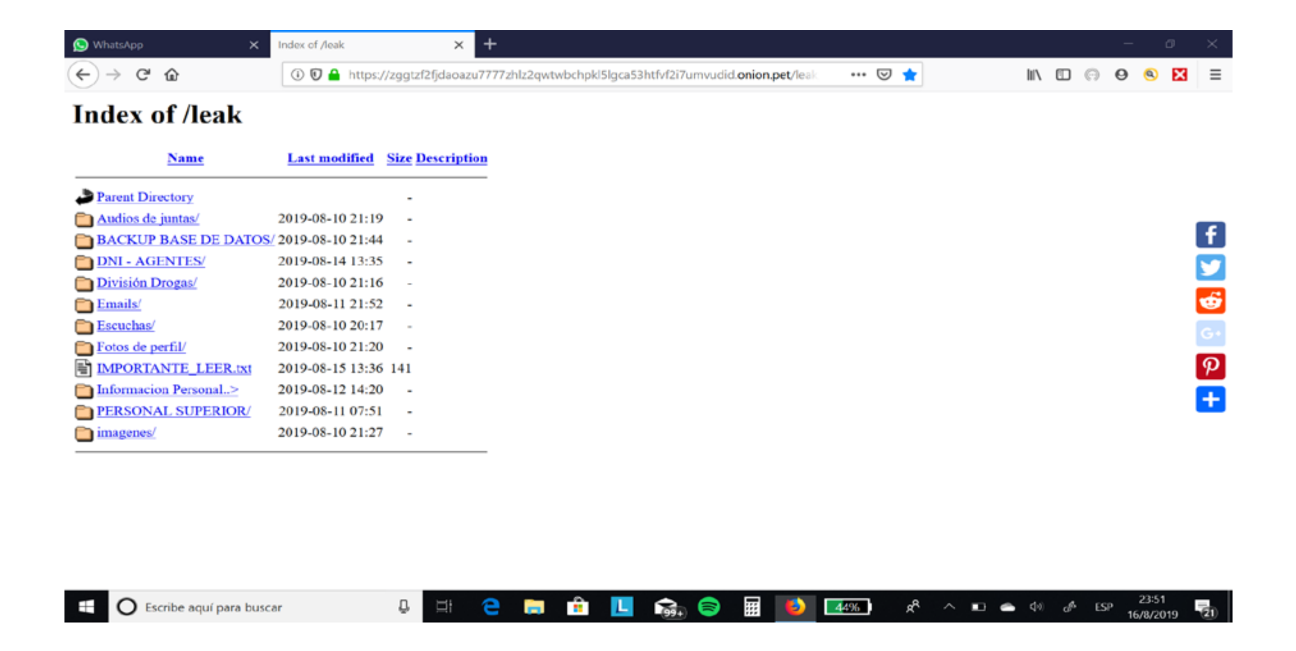
El área de Drogas Peligrosas: Informó que no pudo determinar a la fecha tipo y cantidad de datos personales, por no contar aún con la totalidad de la información compartida en internet.

El área de personal: al día de la fecha no informó tipo y cantidad de datos filtrados.

Hasta el momento esta Sección CIBERSEGURIDAD, no ha podido descargar para su análisis la totalidad de la información filtrada en la Deep Web, debido a que la tasa de transferencia para descarga en muy baja. No obstante, de lo que se desprende de lo visualizado existen gran cantidad de archivos de uso interno y administrativo de distintas dependencias, (.doc, pdf, xls, .rar , jpg, mp4, wav entre otros) que tuviera almacenados en los servicios de almacenamiento en la nube y los propios en discos rígidos internos ya anteriormente explicados.

En relación con información con contenido de datos personales, ampliando lo informado por el área de Bienestar, se observa que, la carpeta identificada en la Deep Web como "DIVISION DROGAS, ESCUCHAS", se hizo un muestreo y se verificó la filtración de 39 fichas con datos y fotos del personal de esa Superintendencia. Respecto a datos con imágenes foto carnet 4x4 de uniforme para uso credencial; DNI escaneados de oficiales en condiciones de ascenso del año 2017; escaneo n° de control credenciales de grado; bases de datos del año 2017 con usuarios y contraseñas sistema "PERSUP"; audios de juntas ascenso, entre otros se encuentran en la carpeta "PERSONAL SUPERIOR, DNI AGENTES, FOTOS DE PERFIL, AUDIO DE JUNTA, BACKUP BASE DE DATOS" del área de personal, hasta el momento no se puede determinar cantidad exacta de los datos filtrados.

A continuación, se procede a adjuntar captura de pantalla de los directorios que se subieron en la Deep Web:



Con respecto a la información filtrada en la Deep Web, desde el día Lunes 02 de septiembre del corriente año, no se encuentra disponible.



República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2019-80081802-APN-SCIB#PFA

CIUDAD DE BUENOS AIRES
Miércoles 4 de Septiembre de 2019

Referencia: REQUERIMIENTO DIRECTOR AAIP-INCIDENTE-PROTECCION DE DATOS PERSONALES

El documento fue importado por el sistema GEDO con un total de 10 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.09.04 13:54:06 -03'00'

Diego Hernan Vituzzi
Jefe de Sección Subcomisario
Sección Ciberseguridad
Policía Federal Argentina

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.09.04 13:54:07 -03'00'